It almost went by unnoticed. On April 3rd, 2014, most news outlets were poring over the EU Parliament's approval of net neutrality and the ending of roaming charges. On that same day, however, the EU Parliament also voted on the proposed 'Regulation on electronic identification and trust services for electronic transactions in the internal market'.

This Regulation, sometimes also referred to as the 'eIDAS Regulation' (**e**lectronic **ID**entification and **A**uthentication **S**ervices), is intended to promote interoperability of national electronic identification (eID) schemes and trust services across the EU. It will also repeal and replace the current eSignature Directive (1999/93/EC).

The European Commission proposed its draft of the eIDAS Regulation on 4 June 2012 and, after several amendments in February 2014, a political agreement was reached between representatives of the European Parliament (MEP), the Commission and the Council. The proposed Regulation was adopted by the MEP with 534 votes in favor, 73 against and 7 abstentions on the 3rd of April 2014. The Regulation is due to be formally endorsed by the Council of Ministers in June.

National eID schemes

Many governmental services require identification of their intended recipients. Filing a tax return, applying for a permit, or requesting a social security benefit all imply identification. Online delivery of these services requires mechanisms to verify identity remotely. This is where electronic identity (eID) schemes come into play.

Today, most European countries have developed – or at least launched the development of – a national identity management strategy. One of the primary objectives of these strategies is to enable remote identification and authentication of citizens. In keeping with this objective, several Member States have moved from purely paper-based identification documents towards electronic identity (eID) cards. However, not all European countries have adopted this approach (see OECD 2011). As a result, there are a wide variety of identification and authentication mechanisms out there. And while diversity is generally a good thing, it may complicate efforts towards the development of Pan-European e-Government Services (PEGS).

Why the Regulation?

Most Member States currently do not recognize foreign eID schemes. As a result, citizens typically can't use their national eIDs to authenticate themselves towards the public administrations of other Member States This poses a barrier for all cross-border online services which require secure identification and authentication, such as cross-border healthcare (see e.g. epSOS) or online public procurement (see e.g. Peppol).

Pan-European eID Interoperability

The eIDAS Regulation does not introduce a common European electronic identification system. Instead, it provides for the possibility of cross-border use and mutual recognition of existing national systems. Under the Regulation, Member States will have the ability to notify their national eID schemes to the Commission. The notification is optional, but once it has been made other Member States are obliged to accept it if their own online public services can be accessed using electronic identification means.

Not all eID schemes support the same level of assurance (LoA). Member States may not want to accept less secure means of authentication for services which require a high level of assurance (e.g., filing a tax return). To resolve this issue, article 8 of the Regulation defines for 3 'Identity assurance levels': 'low', 'substantial' and 'high'. The obligation to recognise the eID schemes of an other Member State will only concern schemes which provide anlevel of identity assurance which is equivalent or higher to the level required for the service in question. This means that it will not possible to access a high value service with low level identification means. The details of these different Identity assurance levels will be worked out further in delegated acts.

The Regulation also foresees the development of an EU interoperability framework. This framework would specify, inter alia, minimum technical requirements for interoperability as well as common security standards. The Regulation explicitly provides that this framework must ensure that personal data is processed in accordance with Directive 95/46/EC and faciliate the implementation of privacy by design.

Trust services

The eIDAS Regulation addresses more than just electronic identification. A second important object of the Regulation concerns trust services. In the Regulation, a trust service is defined as "an electronic service normally provided for remuneration which consists in:

(a) The creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to these services or
(b) The creation, verification and validation of certificates for website authentication or
(c) The preservation of electronic signatures, seals or certificates related to these services."[1]

To be "qualified" or not to be "qualified" …: is that the question?

Just as the eSignature Directive before it, the eIDAS Regulation also differentiates between 'normal', 'advanced' (for electronic signatures and electronic seals) and 'qualified' trust services. The main difference lies in the legal effect of the trust service, which means that for example a 'qualified' electronic signature must be given the equivalent legal effect of a handwritten signature.

However, the non-discrimination rule (introduced by article 5(2) of the eSignature Directive) has also been retained in the eIDAS Regulation. This rule stipulates that a trust service may not be denied legal effect or admissibility solely on the grounds that it is in electronic form or does not meet the

[1] art. 3 (15) Draft eIDAS Regulation.

requirements of a ‘qualified’ service. This rule extends to all of the aforementioned trust services, except qualified certificates for website authentication. And, as before, it will be the national evidentiary rules of Member States which determine what the legal effect shall be of a particular trust service (unless the Regulation explicitly states this effect).

In order to become the provider of a ‘qualified’ trust service, one must formally submit an application to the national supervisory authority. This authority will then verify that all the requirements of the Regulation have been met. Once this verification is complete, the qualified trust service shall be included in national ‘trusted lists’, which shall indicate the qualified status of the service (or service provider) in question. The provider of a qualified trust service shall also be allowed to indicate this status by displaying an EU trustmark. The presentation, composition, size and design of the EU trust mark for qualified trust services shall be specified by way of implementing acts..

What’s next?

The Council is expected to approve the eIDAS regulation in June. The Commission hopes that this Regulation will eventually increase the trust in online environments and promote interoperability national eID schemes. While enhancing such interoperabililty is a generally a good idea, it has yet to be seen whether the Regulation will work in practice. While the eIDAS Regulation provides a legal architecture, technical interoperabilty of European eID schemes will depend most likely depend on implementation project such as STORK 2.0 and FutureID.